REMARKS

This Amendment responds to the Office Action mailed October 3, 2006 in the above-identified application. Based on the foregoing amendments and the following comments, reconsideration and allowance of the application are respectfully requested.

Claims 1-20 were previously pending in the application. By this amendment, claims 6, 9, 10, 12 and 18 have been amended. Claims 7, 8, 13-16, 19 and 20 have been canceled without prejudice or disclaimer. Accordingly, claims 1-6, 9-12, 17 and 18 are currently pending, with claims 1, 4, 6, 12 and 18 being independent claims. No new matter has been added.

The Examiner has rejected claims 1-20 under 35 U.S.C. §103(a) as unpatentable over Sato et al. (US 5,734,855), in view of Philipp (DE 19936890). The rejection is respectfully traversed in view of the amended claims.

Sato discloses a data processor in which a temporary register is used to store the result of an operation before the result is transferred to a destination register (Fig. 2 and col. 2, lines 14-57). However, Sato does not disclose storing a random number in the destination register for masking the operation. Further, Sato does not describe a cryptographic or masking problem.

Philipp discloses a cryptographic operation which provides for a data bit word generated on the basis of random numbers to be stored in a memory cell or a register before a data bit word is written into the same (Abstract).

Claim 1 is directed to an integrated circuit implementing at least one operator involving at least one secret quantity, and functionally comprising upstream and downstream of the operator at least one source register and at least one destination register, respectively, at least one temporary register to store a content of the source register or a result of the operator before transfer to the destination register, and means for loading a random or pseudo-random number at least into the destination register.

As acknowledged by the Examiner, Sato fails to disclose or suggest loading a random number into the destination register, as required by claim 1. The Examiner relies upon Philipp for the teaching that is lacking in Sato. However, Sato has no relation whatever to a cryptographic computation which involves a secret quantity. Thus, one of ordinary skill in the art would have no reason to search beyond Sato for solutions in the field of cryptographic

computation or to refer to Philipp for such solutions. It is respectfully submitted that the combination of Sato and Philipp is based on knowledge of Applicants' invention rather than the teachings of the references themselves. For these reasons, the combination of references is improper and should be withdrawn. Accordingly, claim 1 is patentable over Sato in view of Philipp.

Claims 2 and 3 depend from claim 1 and are patentable over Sato in view of Philipp for at least the same reasons as claim 1.

Claim 4 is directed to an anti-fraud method comprising randomizing a content of a destination register of a result of an operator involving at least one secret quantity, and inputting a random quantity in the destination register before each loading of a result therein, the result of the operator being transferred to a temporary register before loading into the destination register.

Sato contains no disclosure or suggestion of an anti-fraud method comprising randomizing a content of a destination register of a result of an operator involving at least one secret quantity nor of inputting a random quantity in the destination register, as required by claim 4. Sato is unrelated to cryptographic computation. Accordingly, the skilled person would have no reason to combine the teachings of Sato and Philipp to provide the anti-fraud method of claim 4. For these reasons and for the reasons discussed above, the combination of references is improper, and withdrawal of the rejection is respectfully requested.

Claim 5 depends from claim 4 and is patentable over Sato in view of Philipp for at least the same reasons as claim 4.

Amended claim 6 is directed to an integrated circuit comprising an operator configured to perform an operation on a secret quantity, a destination register coupled to receive a result of the operation, a control circuit configured to load a random or pseudo-random number into the destination register before transfer of the result into the destination register, to protect against attacks by physical signature analysis, a source register coupled to provide data to the operator, and a temporary register configured to store the data of the source register or the result of the operation, wherein the control circuit is further configured to load a random number or pseudo-random number into the temporary register.

Sato contains no disclosure or suggestion of a control circuit to load a random or pseudo-random number into a destination register to protect against attacks by physical signature

analysis, as required by claim 6. Further, neither cited reference discloses a control circuit configured to load a random or pseudo-random number into a temporary register, as required by claim 6. Because Sato is unrelated to cryptographic computation, the skilled person would have no reason to combine the teachings of Sato and Philipp. For at least these reasons, amended claim 6 is clearly and patentably distinguished over Sato in view of Philipp, and withdrawal of the rejection is respectfully requested.

Claims 9-11 depend from claim 6 and are patentable over Sato in view of Philipp for at least the same reasons as claim 6.

Amended claim 12 is directed to an antifraud method comprising randomizing a content of a destination register coupled to receive a result of an operation involving a secret quantity before transfer of a result into the destination register, to protect against attacks by physical signature analysis, wherein randomizing the content of a destination register comprises loading a random or pseudo-random number into a temporary register, transferring the result of the operation to the temporary register, loading a random or pseudo-random number into the destination register and transferring the result from the temporary register to the destination register.

Sato is unrelated to cryptographic computation and contains no disclosure or suggestion of randomizing a content of a destination register to protect against attacks by physical signature analysis, as required by claim 12. Further, neither cited reference discloses loading a random or pseudo random number into a temporary register, transferring the result of the operation to the temporary register, loading a random or pseudo random number into the destination register and transferring the result from the temporary register to the destination register, as required by amended claim 12. In addition, the skilled person would have no reason whatever to combine the teachings of Sato and Philipp, since Sato is unrelated to cryptographic computation. For at least these reasons, amended claim 12 is clearly and patentably distinguished over Sato in view of Philipp, and withdrawal of the rejection is respectfully requested.

Claim 17 depends from claim 12 and is patentable over Sato in view of Philipp for at least the same reasons as claim 12.

Amended claim 18 is directed to an antifraud method comprising performing an operation on a secret quantity to produce a result, loading a random or pseudo-random number

into a destination register that is coupled to receive the result of the operation, to protect against attacks by physical signature analysis, loading a random or pseudo-random number into a temporary register, transferring the result of the operation to the temporary register, and transferring the result of the operation from the temporary register to the destination register.

Amended claim 18 is patentable over Sato in view of Philipp for at least the reasons discussed above in connection with claims 6 and 12. Accordingly, withdrawal of the rejection is respectfully requested.

Based upon the above discussion, claims 1-6, 9-12, 17 and 18 are in condition for allowance.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: January 3, 2007

Respectfully submitted,

By: William R. McClellan

William R. McClellan
Registration No.: 29,409
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000

x01/03/2006x